Discrete Mathematics 92 (1991) 145–158
North-Holland

Laws in a class of groupoids

Ann Chi Kim*

Department of Mathematics, Pusan National University, Pusan 607, Korea

B.H. Neumann

Department of Mathematics, Australian National University, Canberra, A.C.T. 2601, Australia

Received 1 July 1988
Revised 25 November 1988

Dedicated to Professor R.G. Stanton on the occasion of his 68th birthday.

Abstract

Kim, A.C. and B.H. Neumann, Laws in a class of groupoids, Discrete Mathematics 92 (1991) 145–158.

The laws of a class of groupoids are investigated, and shown to have no finite basis.

1. Introduction

In an earlier paper [2] a class of groupoids was described, and it was shown that the laws in a typical one of them have no finite basis; and the question was asked what laws hold simultaneously in the whole class. This question motivates the present investigation. Knowledge of the earlier paper is not assumed.

Let $\mathcal{S}$ be an arbitrary commutative semigroup, written additively, with carrier S, and α and β two commuting endomorphisms of $\mathcal{S}$, written as right-hand operators. We define a new binary operation μ on S by

$$xy\mu = x\alpha + y\beta.$$

Then S becomes the carrier of a groupoid, denoted by $\mathcal{G}(\alpha, \beta)$, or $\mathcal{G}$ for short. Our object is to study the laws of $\mathcal{G}$ that do not depend on the particular semigroup $\mathcal{S}$, nor on the particular endomorphisms α and β. The shortest nontrivial law is the *medial* law

$$xy\mu zt\mu^2 = xz\mu yt\mu^2$$

* The first author thanks the Korea Science and Engineering Foundation for financial support, and Miss Jeong Young Kim for assistance with some of the computations involved.

(where μ^2 stands for $\mu\mu$, and μ^n is similarly an abbreviation for n repetitions of μ). This has consequences that are longer laws; we are here interested in those laws that are not consequences of the medial law, and we shall exhibit an infinite sequence of such laws. The main result is that there is no finite basis for the laws of the groupoids here considered.

2. Preliminaries

Before we describe the laws of the groupoids we are here interested in, we put together some simple (known) facts on laws in groupoids. The facts are valid more generally, but we list them only for groupoids, the groupoid operation being denoted by μ and written as right-hand operator.

The laws

$$\mathscr{L}_0 \qquad w = w$$

are the 'trivial' laws. All other laws are of the form $w = w'$, where w, w' are distinct words in 'variables' $x_1, x_2, x_3, \ldots$ (or $x, y, z, \ldots$) and μ. (The words in the variables form a free groupoid $\mathscr{F}$.) The *length* $\lambda(w)$ of a word w is the number of variables (counted with multiplicities if repeated) in it; it is always 1 plus the number of occurrences of μ in w. The length $\lambda(w = w')$ is defined as the smaller of the lengths of the two words,

$$\lambda(w = w') = \min(\lambda(w), \lambda(w')).$$

If $\lambda(w = w') = \lambda(w) = \lambda(w')$, the law $w = w'$ is an *equal length law*.

If $\mathscr{L}$ is a set of laws valid in a groupoid, we define the set $\mathscr{L}^*$ of *consequences* of $\mathscr{L}$ (also known as the *closure* of $\mathscr{L}$) as follows:

(2.1) The laws in $\mathscr{L}$ are consequences of $\mathscr{L}$.

(2.2) The trivial laws $\mathscr{L}_0$ are consequences of $\mathscr{L}$.

(2.3) If $w = w'$ is a consequence of $\mathscr{L}$, then $w' = w$ is a consequence of $\mathscr{L}$.

(2.4) If $w = w'$ and $w' = w''$ are consequences of $\mathscr{L}$, then $w = w''$ is a consequence of $\mathscr{L}$.

(2.5) If $u = u'$ and $v = v'$ are consequences of $\mathscr{L}$, then $uv\mu = u'v'\mu$ is a consequence of $\mathscr{L}$.

(2.6) Let ε be a mapping of the variables into the carrier S of $\mathscr{G}$. Thus each $x_i\varepsilon$ is a word in the variables. If w is a word, denote by $w\varepsilon$ the word obtained from w by substituting $x_i\varepsilon$ for each x_i. Then if $w = w'$ is a consequence of $\mathscr{L}$, then $w\varepsilon = w'\varepsilon$ is a consequence of $\mathscr{L}$. (The mapping ε can be extended to an endomorphism of $\mathscr{G}$.)

(2.7) Consequences of consequences of $\mathscr{L}$ are consequences of $\mathscr{L}$.

A law that is not in the set $\mathscr{L}^*$ of consequences of $\mathscr{L}$ is said to be *independent* of $\mathscr{L}$.

In universal algebra parlance, if we consider the set of groupoid words as the free groupoid $\mathscr{F}$ of countably infinite rank, then $\mathscr{L}$ is a relation on $\mathscr{F}$, and $\mathscr{L}^*$ is the fully invariant congruence relation on $\mathscr{F}$ generated by $\mathscr{L}$. The trivial laws $\mathscr{L}_0$ form the least such congruence, corresponding to the diagonal of $\mathscr{F} \times \mathscr{F}$, and $\mathscr{L}_0^* = \mathscr{L}_0$.

The following lemma will be used to show independence of laws.

Lemma 2.8. *If the equal length law $w_1 = w_1'$ is a nontrivial consequence of the set $\mathscr{L}$ of laws, then it is a consequence of 'shorter' nontrivial laws in $\mathscr{L}$, that is to say laws $w = w'$ with*

$$\lambda(w = w') \leq \lambda(w_1 = w_1').$$

Proof. This is immediately seen from the definition (2.1)–(2.7) of consequences. Note that there is no unit element (or empty word) available for substitution in (2.6)—the lemma would otherwise be false. $\square$

3. Words, evaluation, and matrices

As we are interested in the laws of $\mathscr{G}$ that do not depend on the semigroup $\mathscr{S}$ nor on the endomorphisms α, β, we may take $\mathscr{S}$ to be the free commutative semigroup on a countable set of generators $x_1, x_2, x_3, \ldots$ and the endomorphisms α, β to be 'freely commuting', that is to say such that $\alpha\beta = \beta\alpha$, but that

$$\alpha^a\beta^b = \alpha^c\beta^d$$

only if $a = c$ and $b = d$, and that there are no other relations between them. This ensures that every equation valid in $\mathscr{G}$ is a law in $\mathscr{G}$, and in the whole class of such groupoids.

If w is an element of $\mathscr{G}$, that is to say a word in the elements of S operated on by μ, then w can be evaluated in $\mathscr{S}$ to give an element $P(w)$. This will be a sum of terms $x_i\gamma_i$, where the γ_i are polynomials in α and β. If for two words w, w' this evaluation gives the same result

$$P(w) = P(w')$$

then $w = w'$ is a law in $\mathscr{G}$. For example, if

$$w = x_1x_2\mu x_3x_4\mu^2, \qquad w' = x_1x_3\mu x_2x_4\mu^2,$$

then

$$P(w) = x_1\alpha^2 + x_2\alpha\beta + x_3\beta\alpha + x_4\beta^2,$$

$$P(w') = x_1\alpha^2 + x_3\alpha\beta + x_2\beta\alpha + x_4\beta^2,$$

because addition in $\mathscr{S}$ is commutative and α and β also commute; we thus get the medial law (Etherington [1] calls this the *entropic* law, Murdoch [3] in the case of a quasigroup uses the term *Abelian*):

$$x_1x_2\mu x_3x_4\mu^2 = x_1x_3\mu x_2x_4\mu^2 \tag{3.1}$$

mentioned in the introduction.

We note two features of the medial law (3.1). It is an equal length law, and all variables on each side are distinct, or, differently put, the number n of variables equals the length

$$\lambda(w = w') = \lambda(w) = \lambda(w') = n. \tag{3.2}$$

The first of these features is common to all laws of $\mathscr{G}$. In fact a stronger fact is easily proved.

Lemma 3.3. If $w = w'$ *is a law in* $\mathscr{G}$, *then every variable that occurs* k *times in* w *occurs also* k *times in* w'.

Proof. To see this we simply note that if the variable x occurs k times in w, then its coefficient in $P(w)$ is a sum of k monomials in α, β. $\square$

The second feature is not common to all laws of $\mathscr{G}$; for example, the medial law entails the law

$$x_1x_1\mu x_2x_2\mu^2 = x_1x_2\mu x_1x_2\mu^2$$

in only 2 variables. However, in the sequel we shall concentrate on laws that have the property (3.2), that is to say in which the variables on each side are distinct. We call such laws *distinct variable laws*.

Let w be a word in which all variables are distinct; we may assume the variables to be $x_1, x_2, \ldots, x_n$, where $n = \lambda(w)$. Then on evaluation we obtain an expression in which the coefficient of each variable x_i is a monomial in α, β, that is to say of the form

$$P(w) = \sum_{i=1}^{n} x_i\alpha^{a_i}\beta^{b_i},$$

where the exponents a_i, b_i are nonnegative integers. We associate with $P(w)$ the $2 \times n$ matrix $M(w)$ of these exponents,

$$M(w) = \begin{bmatrix} a_1a_2 \cdots a_n \\ b_1b_2 \cdots b_n \end{bmatrix}.$$

The matrix $M(w)$ can be computed inductively by the following rules:

(3.41) If $\lambda(w) = 1$, that is $w = x_1$, then

$$M(w) = \begin{bmatrix} 0 \\ 0 \end{bmatrix};$$

(3.42) If $\lambda(w) > 1$, so that $w = uv\mu$ and $\lambda(w) = \lambda(u) + \lambda(v)$, and if

$$M(u) = \begin{bmatrix} c_1c_2\cdots c_l \\ d_1d_2\cdots d_l \end{bmatrix}, \qquad M(v) = \begin{bmatrix} e_1e_2\cdots e_m \\ f_1f_2\cdots f_m \end{bmatrix},$$

then

$$M(w) = \begin{bmatrix} c_1+1 & c_2+1 & \cdots & c_l+1 & e_1 & e_2 & \cdots & e_m \\ d_1 & d_2 & \cdots & d_l & f_1+1 & f_2+1 & \cdots & f_m+1 \end{bmatrix}.$$

For future reference we turn this second rule round:

(3.43) If $\lambda(w) = n > 1$, and if

$$M(w) = \begin{bmatrix} a_1a_2\cdots a_n \\ b_1b_2\cdots b_n \end{bmatrix}, \tag{3.43.1}$$

then, for some $l < n$, $w = uv\mu$, where $\lambda(u) = l$, $\lambda(v) = m = n - l$, and

$$M(u) = \begin{bmatrix} a_1-1 & a_2-1 & \cdots & a_l-1 \\ b_1 & b_2 & \cdots & b_l \end{bmatrix},$$

$$M(v) = \begin{bmatrix} a_{l+1} & a_{l+2} & \cdots & a_n \\ b_{l+1}-1 & b_{l+2}-1 & \cdots & b_n-1 \end{bmatrix}.$$

We note in passing that in the matrix (3.43.1) always $b_1 = a_n = 0$, and all other entries a_i, b_i are positive and less than n; also if a number a appears in the first row, then $a-1$ also appears, further to the right; and if b appears in the second row, then also $b-1$, further to the left. These facts are easily proved inductively from (3.41) and (3.42). They severely restrict the matrices that can be of the form $M(w)$, but there appears no obvious way, other than repeated application of (3.43) if possible, to decide whether a given $2 \times n$ matrix is of the form $M(w)$.

In order to apply (3.43) to a given matrix, we have to find the length of u and v; for this we can use the following rule, derived easily from (3.43):

(3.44) If $\lambda(w) = n > 1$, then $M(w)$ contains a unique 2×2 submatrix of the form

$$\begin{bmatrix} a_la_{l+1} \\ b_lb_{l+1} \end{bmatrix} = \begin{bmatrix} 1 & q \\ p & 1 \end{bmatrix}.$$

Then $w = uv\mu$ where $\lambda(u) = l$.

We exhibit, as an example, the matrices for words of small length.

$$\lambda = 1: \qquad M(x_1) = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

$$\lambda = 2: \qquad M(x_1x_2\mu) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\lambda = 3: \qquad M(x_1x_2\mu x_3\mu) = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \qquad M(x_1x_2x_3\mu^2) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \end{bmatrix}.$$

For $\lambda = 4$ there are 5 matrices, for $\lambda = 5$ there are 14, and generally for $\lambda = n$ there are C_n matrices, where C_n is the nth Catalan number.

The matrix of $w = x_1x_2\mu x_3x_4\mu^2$ is

$$M(x_1x_2\mu x_3x_4\mu^2) = \begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

Because the two middle columns, corresponding to x_2 and x_3, are equal, interchanging x_2 and x_3 must give the same matrix, and thus the same evaluation polynomial $P(w)$. Thus these two equal columns signal the medial law. More generally we have the following useful fact.

Lemma 3.5. *Let w be such that in $M(w)$ the ith and jth columns are equal, and let w' be the word obtained from w by interchanging x_i and x_j. Then $w = w'$ is a law in $\mathcal{G}$.*

We omit the (easy) proof.

More generally we have the following fact.

Theorem 3.6. *Let w be a word in distinct variables $x_1, x_2, \ldots, x_n$ (so that $\lambda(w) = n$), and let w' be a word such that $w = w'$ is a law in $\mathcal{G}$. Let the matrices of w and w' be*

$$M(w) = \begin{bmatrix} a_1a_2\cdots a_n \\ b_1b_2\cdots b_n \end{bmatrix}, \qquad M(w') = \begin{bmatrix} a_1'a_2'\cdots a_n' \\ b_1'b_2'\cdots b_n' \end{bmatrix}.$$

Then there is a permutation π of $(1, 2, \ldots, n)$ such that for each i the ith column

$$\begin{bmatrix} a_i' \\ b_i' \end{bmatrix} \quad \text{of} \quad M(w')$$

equals the $i\pi$th column

$$\begin{bmatrix} a_{i\pi} \\ b_{i\pi} \end{bmatrix} \quad \text{of} \quad M(w).$$

Conversely, if there is such a permutation π, then $w = w'$ is a law in $\mathcal{G}$.

Proof. The variables in w' must be the same as those in w (see Lemma 3.3). Thus the variables $x_1, x_2, \ldots, x_n$ occur in w' in some permuted order, say $x_{1\pi}, x_{2\pi}, \ldots, x_{n\pi}$. Now write $P(w)$ and $P(w')$ as sums of the variables as they occur, with the appropriate monomials in α, β as coefficients:

$$P(w) = x_1\alpha^{a_1}\beta^{b_1} + x_2\alpha^{a_2}\beta^{b_2} + \cdots + x_n\alpha^{a_n}\beta^{b_n},$$
$$P(w') = x_{1\pi}\alpha^{a_1'}\beta^{b_1'} + x_{2\pi}\alpha^{a_2'}\beta^{b_2'} + \cdots + x_{n\pi}\alpha^{a_n'}\beta^{b_n'}.$$

As $w = w'$ is a law in $\mathcal{G}$, we must have $P(w) = P(w')$. Thus if $i\pi = j$, then $a_i' = a_j$, $b_i' = b_j$. Conversely, if there is a permutation of the columns of $M(w')$ giving those of $M(w)$, then $P(w) = P(w')$, and $w = w'$ is a law in $\mathcal{G}$. $\square$

As an example consider

$$w = x_1x_2x_3\mu^2x_4x_5\mu^2, \qquad w' = x_1x_4\mu x_2x_3\mu x_5\mu^2.$$

Then

$$M(w) = \begin{bmatrix} 2 & 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 \end{bmatrix}, \qquad M(w') = \begin{bmatrix} 2 & 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 2 \end{bmatrix},$$

and the permutation $\pi = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{smallmatrix}\right] = (2\,4\,3)$ (in cyclic notation) is as in the theorem. Thus $w = w'$ is a law in $\mathscr{G}$. It is obtained from the medial law by the substitution ε defined by $x_1\varepsilon = x_1$, $x_2\varepsilon = x_2x_3\mu$, $x_3\varepsilon = x_4$, $x_4\varepsilon = x_5$ (the remaining variables do not matter).

4. Dependence and independence of laws

By comparing the matrices that belong to the words of length $\leqslant 4$, one easily verifies that the medial law is the shortest nontrivial law, and there is no other nontrivial distinct-variable law of length 4, except of course those obtained from the medial law by renaming the variables.

We now consider nontrivial distinct-variable laws of the form $w = w'$. We may assume, without loss of generality, that the variables in w are $x_1, x_2, \ldots, x_n$, in this order, and that in w' they appear in the order $x_{1\pi}, x_{2\pi}, \ldots, x_{n\pi}$, where π is a permutation of $\{1, 2, \ldots, n\}$.

We note in passing that π must leave 1 and n unchanged, as $b_1 = 0$ and $a_n = 0$ and no other a_i or b_i is zero in $M(w)$, see (3.6). Thus the least n for which a nontrivial permutation π can exist is $n = 4$, and then $\pi = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{smallmatrix}\right]$, or briefly $\pi = (2\ 3)$ is the only candidate: and this indeed occurs, for the medial law.

As n increases, the number of possible permutations rises steeply. We propose, therefore, to concentrate on those laws whose associated permutations are transpositions, say $\pi = (i\,j)$. Let us call such laws *transposition laws*: the medial law is a transposition law, but the example at the end of the last section is not. If $w = w'$ is a transposition law, then $a_i = a_j$ and $b_i = b_j$; and conversely, if $M(w)$ has two equal columns, say the ith and the jth, then $w = w'$ is a transpositional law, where w' is obtained from w by interchanging x_i and x_j.

Thus we make the convention for the rest of this section that w, w', i, j, a_i, b_i have the above meanings, and we further make the convention that

$$i < j, \qquad w = uv\mu, \qquad w' = u'v'\mu,$$

$$\lambda(w) = \lambda(w') = n, \qquad \lambda(u) = l, \qquad \lambda(v) = n - l = m.$$

We first assemble a few obvious facts.

Lemma 4.1. *In a transposition law $w = w'$, $\lambda(u') = \lambda(u)$ and $\lambda(v') = \lambda(v)$.*

Proof. This follows immediately from the rule (3.44) for recognising $\lambda(u)$ from the matrix $M(w)$ which equals $M(w')$. □

Lemma 4.2. *If $j \leq l$, then the law $w = w'$ is a consequence of the shorter law $u = u'$, and if $i > l$, then the law $w = w'$ is a consequence of the shorter law $v = v'$.*

Proof. If $j \leq l$, then both x_i and x_j occur in u, and their interchange only turns u into u'; and similarly if $i > l$. □

We may thus now restrict attention to the case that $i \leq l < j$, so that the interchange of x_i and x_j affects both u and v. Take as an example

$$w = x_1x_2x_3\mu^2x_4x_5\mu x_6\mu^2.$$

Then

$$M(w) = \begin{bmatrix} 2 & 2 & 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 & 2 \end{bmatrix},$$

with the second and fourth columns (and also the third and fifth columns) equal. Thus putting

$$w' = x_1x_4x_3\mu^2x_2x_5\mu x_6\mu^2,$$

we obtain the transposition law

$$w = w'; \tag{4.31}$$

and if we put

$$w'' = x_1x_2x_5\mu^2x_4x_3\mu x_6\mu^2,$$

we obtain another transposition law

$$w = w''. \tag{4.32}$$

If we apply both transpositions, we get the word

$$w^* = x_1x_4x_5\mu^2x_2x_3\mu x_6\mu^2,$$

and from this the law (not a transposition law)

$$w = w^*. \tag{4.33}$$

While each of the laws (4.31) and (4.32) is independent of all shorter laws (and, by Lemma 2.8, also of all longer laws), (4.33) is a consequence of the medial law, obtained by substituting $x_2x_3\mu$ for x_2 in (3.1), $x_4x_5\mu$ for x_3 and changing x_4 to x_6. Thus the law (4.32) follows from the medial law (3.1) jointly with (4.31), and similarly (4.31) follows from (3.1) and (4.32).

Our assertion that (4.31) is independent of all shorter laws will follow from more general independence criteria later. For the present we just notice one feature of our example, namely that all the 'factors' u, v, u', v', u'', v'', u^*, v^* of w, w' w'', w^* have the same length $l = m = \cdots = 3$. As we shall see later, this is no coincidence.

5. Dependence of transposition laws

To develop criteria for a transposition law to be independent of shorter laws, we first have to refine Lemma 4.1. This requires some definitions.

Definition 5.11. The only *subword* of a variable is that variable itself. Let w be a word of length $\lambda(w) = n > 1$, and assume that, for words of length $<n$, *subwords* have already been defined. Put $w = uv\mu$. Then the *subwords* of w are w itself and all subwords of u and v. A *proper* subword of w is a subword of w other than w itself.

Definition 5.12. Let w be a word in distinct variables and s a subword. The *signature* $\sigma(w, s)$ of s in w is a sequence $(\sigma_1, \sigma_2, \ldots)$ of symbols λ and ρ ('left' and 'right') defined inductively by:

(5.12.1) $\sigma(w, w) = (\ )$, the empty sequence;

(5.12.2) If $w = uv\mu$ and s is a subword of u with signature $\sigma(u, s) = (\tau_1, \tau_2, \ldots)$, then $\sigma(w, s) = (\lambda, \tau_1, \tau_2, \ldots)$; if s is instead a subword of v with signature $\sigma(v, s) = (\tau_1, \tau_2, \ldots)$, then $\sigma(w, s) = (\rho, \tau_1, \tau_2, \ldots)$. If s' is a subword of w' and if $\sigma(w', s') = \sigma(w, s)$, then s' is *homologous* to s.

The signature thus describes the way to get from a word to a subword by taking a sequence of left or right factors. We can now extend Lemma 4.1.

Lemma 5.2. *If $w = w'$ is a transposition law and if s, s' are homologous subwords of w, w', respectively, then $\lambda(s') = \lambda(s)$, and moreover, $M(s) = M(s')$.*

Proof. We have already noted that u and u' (and also v and v') have the same length. Applying (3.43), we see that they must also have equal matrices. Induction over the length of the signature completes the argument. □

Lemma 5.3. *Let $w = w'$ be a transposition law and s a proper subword of w of length >1; let $s = s_1s_2\mu$. If both $\lambda(s_1) > 1$ and $\lambda(s_2) > 1$, then $w = w'$ is a consequence of a shorter law.*

Proof. By Lemma 4.2 we may assume without loss of generality that at most one of x_i, x_j occurs in s; thus in at least one of s_1, s_2 neither x_i nor x_j occurs, say in s_2. Put $s^{\#} = s_1y\mu$, where y is a new variable; if $s' = s_1's_2'$ is the subword of w' homologous to s, then $s_2' = s_2$, and we put $s'^{\#} = s_1'y\mu$. Now denote by $w^{\#}$ and $w'^{\#}$

the words obtained from w, w', respectively, by replacing s by $s^\#$ and s' by $s'^\#$. Then $w^\# = w'^\#$ is also a transposition law, shorter than our original one, and we retrieve the original law by substituting s_2 for y. (One needs to satisfy oneself that in $M(w^\#)$ and $M(w'^\#)$ the variables that correspond to x_i and x_j in w and w' again have the same columns; we omit the argument.) The case that x_i or x_j occurs in s_2 (and thus neither occurs in s_1) is similar. □

Corollary 5.4. *If $w = w'$ is a transposition law which is independent of shorter laws, with $w = uv\mu$ and $w' = u'v'\mu$, then there are sequences of subwords $u_1, u_2, \ldots, u_l = u$, $v_1, v_2, \ldots, v_m = v$, $u'_1, u'_2, \ldots, u'_l = u'$, $v'_1, v'_2, \ldots, v'_m = v'$, such that each u'_k is homologous to u_k and each v'_k to v_k, each u_k and v_k is of length k, and if $k < l$, then*

$$u_{k+1} = u_k x\mu \quad \text{or} \quad u_{k+1} = xu_k\mu,$$

where x is one of the variables, and similarly for u'_{k+1} and for v_{k+1}, v'_{k+1} if $k < m$.

This corollary severely restricts the words that can occur in a transposition law that is not dependent on shorter laws. It also allows us to locate the transposing variables x_i and x_j more accurately.

Lemma 5.5. *With the conventions and notation of Corollary 5.4, $u_1 = x_i$ or $u_2 = u_1x_i\mu$ or $u_2 = x_iu_1\mu$, and $v_1 = x_j$ or $v_2 = v_1x_j\mu$ or $v_2 = x_jv_1\mu$.*

Proof. Assume, on the contrary, that x_i occurs only later, so that $u_{k+1} = u_kx_i\mu$ or $u_{k+1} = x_iu_k\mu$, with $k > 1$. Replace u_k by a new variable y, to obtain a new word $w^\#$, shorter than w. Now the subword u'_{k+1} of w' homologous to u_{k+1} will be, correspondingly, $u'_{k+1} = u'_kx_j\mu = u_kx_j\mu$, or $u'_{k+1} = x_ju'_k\mu = x_ju_k\mu$, and here we also replace u_k by y, to get a new word $w'^\#$. Clearly $w^\# = w'^\#$ is a transposition law, shorter than our original law, which follows from it by the substitution of u_k for y. The rest of the argument, dealing with v, is analogous. □

Now the matrix $M(u_2) = \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$, as also the matrix $M(v_2)$, which is the same, has the property that the column sums equal 1; and as in each step from u_k to u_{k+1} and in each step from v_k to v_{k+1} a single column is attached to the matrix (see Corollary 5.4), these particular two columns have a 1 added in the first or second row at each such step. These columns are those of x_i and $x_{i\pm1}$ and of x_j and $x_{j\pm1}$, respectively, and thus the column sum corresponding to x_i in $M(u_k)$, and the column sum corresponding to x_j in $M(v_k)$, equals always $k-1$. The column sum of x_i in $M(u) = M(u_l)$ is $l-1$, and the column sum of x_j in $M(u) = M(u_m)$ is $m-1$. But then the column corresponding to x_i in $M(w)$ has sum l, and that corresponding to x_j in $M(w)$ has sum m. As these two columns are equal, we have the following fact.

Corollary 5.6 *With the conventions and notation of Corollary 5.4, u and v have the same length $\lambda(u) = l = m = \lambda(v)$. In particular if w in a transposition law $w = w'$ has odd length, then the law is a consequence of shorter laws.*

6. The main result

Before we state and prove our main result, we supply ourselves with an infinite sequence of transposition laws. We define, for $m \geqslant 3$,

$$u_m = x_1 x_2 \cdots x_m \mu^{m-1},$$
$$v_m = x_{m+1} x_{m+2} \cdots x_{2m-1} \mu^{m-2} x_{2m} \mu.$$

The matrices are easily computed; they are:

$$M(u_m) = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 2 & \cdots & m-2 & m-1 \end{bmatrix},$$

$$M(v_m) = \begin{bmatrix} 2 & 2 & 2 & \cdots & 2 & 1 & 0 \\ 0 & 1 & 2 & \cdots & m-3 & m-2 & 1 \end{bmatrix}.$$

Thus, putting $2m = n$ and $w_n = u_m v_m \mu$, (so that the suffices of these words represent their length), we get the matrix

$$M(w_n) = \begin{bmatrix} 2 & 2 & 2 & \cdots & 2 & 1 & 2 & 2 & 2 & \cdots & 2 & 1 & 0 \\ 0 & 1 & 2 & \cdots & m-2 & m-1 & 1 & 2 & 3 & \cdots & m-2 & m-1 & 2 \end{bmatrix}.$$

Here we see $m-1$ pairs of equal columns, giving rise to $m-1$ transposition laws; but almost all of them are consequences of shorter laws, by Lemma 5.5. In fact if $m \geqslant 3$, the only pairs of columns that are not excluded from consideration by Lemma 5.5 are the pairs of columns $\left[\begin{smallmatrix} 2 \\ m-2 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 \\ m-1 \end{smallmatrix}\right]$. Thus we look at the transposition law that uses the transposition $\pi = (m-1\ 2m-2)$. Denote by w_n' the word obtained from w_m by interchanging x_{m-1} and x_{2m-2}. Then we propose to show that the transposition law

$$\ell_n': \qquad w_n = w_n'$$

is independent of all shorter laws. We remark that the medial law is not of the form ℓ_4', but that the law (4.31) is ℓ_6'.

Inspection of the rules (2.1)–(2.7) shows that the only rules that might be relevant to deriving ℓ_n' from shorter laws are (2.4), (2.5), and (2.6). However, to apply (2.5) to obtain ℓ_n', we need laws $u = u'$ and $v = v'$; and there can be no such laws, as u and u' do not involve the same variables (nor do v and v').

Next we wish to show that there is no shorter law $\bar{w} = \bar{w}'$ from which $w_n = w_n'$ can be derived by the substitution rule (2.6). There are indeed words $\bar{w}$ that lead to w_n with a suitable substitution: consider the word

$$\bar{w}_{i,j} = x_1 x_2 \cdots x_i y \mu^i x_{m+1} x_{m+2} \cdots x_{m+j} z \mu^j x_n \mu^2,$$

where $1 \leqslant i \leqslant m-1$, $1 \leqslant j \leqslant m-2$. The substitution ε that leaves all x_i unchanged but puts

$$y\varepsilon = x_{i+1}x_{i+2} \cdots x_m \mu^{m-i-1},$$
$$z\varepsilon = x_{m+j+1}x_{m+j+2}x_{n-1}\mu^{m-j-2}$$

will make $\bar{w}_{i,j}\varepsilon = w_n$. Here we interpret μ^0, when $i = m-1$ or $j = m-2$, naturally as the absence of μ. One easily satisfies oneself that there are no essentially different words that will give w_n with a suitable substitution. The matrix of $\bar{w}_{i,j}$ is

$$M(\bar{w}_{i,j}) = \begin{bmatrix} 2 & 2 & \cdots & 2 & 1 & 2 & 2 & \cdots & 2 & 1 & 0 \\ 0 & 1 & \cdots & i-1 & i & 1 & 2 & \cdots & j-1 & j & 2 \end{bmatrix},$$

and inspection shows that the only permutations of the columns that can give rise to a law are transpositions or products of disjoint transpositions. Those that affect only the first i or j columns (according to which of i and j is the smaller) will, after application of the substitution ε, give a law that indeed equates w_n to another word, but not to w_n'. If $i = j$, then $\bar{w}_{i,i} = w_{2i+2}$, and there is an extra pair of columns that can be interchanged, namely the $(i+1)$th column and the penultimate one. After application of ε this gives again a valid law equating w_n with another word, but again this is not w_n', because the pair of variables x_{m-1}, x_m is exchanged for the pair x_{n-2}, x_{n-1}, instead of only the first members of these pairs.

Finally, to show that the transitivity rule (2.4) does not make our law ℓ_n' derivable from shorter laws, we first show a certain uniqueness.

Lemma 6.1. *Let the matrix $M(w)$ of a word w have the same columns, in some order, as $M(w_n)$. Then the matrices are equal, $M(w) = M(w_n)$.*

Proof. We know already that the columns $\left[\begin{smallmatrix}2\\0\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0\\2\end{smallmatrix}\right]$ must be the first and last columns of $M(w)$, respectively. Write $w = uv\mu$. To find out where u ends and v begins, we use (3.44), that is to say, we look for a submatrix $\left[\begin{smallmatrix}1 & ?\\p & 1\end{smallmatrix}\right]$. Now the only value of p that can be found in $M(w_n)$ is $m-1$. It follows that u has length $\lambda(u) \geqslant m$. We turn to v: the fact that the last column of $M(w_n)$ is $\left[\begin{smallmatrix}0\\2\end{smallmatrix}\right]$ shows that $\lambda(v) > 1$; we write $v = v'v''\mu$ and again apply the rule (3.44), to find a submatrix of $M(v)$ of the form $\left[\begin{smallmatrix}1 & ?\\p & 1\end{smallmatrix}\right]$; this time the only value of p that can be found below a 1 is $m-2$, which comes from the $m-1$ below a 1 in $M(w)$. This shows that v' has length $\lambda(v') \geqslant m-1$. Thus also v has length $\lambda(v) \geqslant m$. It follows that $\lambda(u) = \lambda(v) = m$, and the matrices of u and v can now be easily computed, using (3.43),

$$M(u) = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & \cdots & m-2 & m-1 \end{bmatrix} = M(u_m),$$
$$M(v) = \begin{bmatrix} 2 & 2 & \cdots & 2 & 1 & 0 \\ 0 & 1 & \cdots & m-3 & m-2 & 1 \end{bmatrix} = M(v_m).$$

This proves the lemma. $\square$

It follows from this that the only permutations of columns of $M(w_n)$ that again give the matrix of a word are the ones that leave the matrix unchanged, that is the transpositions and products of disjoint transpositions. Now assume we have a sequence of laws $w^{(1)} = w^{(2)}$, $w^{(2)} = w^{(3)}, \ldots, w^{(s-1)} = w^{(s)}$, where $w^{(1)} = w_n$ and $w^{(s)} = w'_n$, and where every law

$$\ell^{(k)}: \qquad w^{(k)} = w^{(k+1)}$$

is a consequence of shorter laws. We know already that all the words $w^{(k)}$ have the same matrix, and all the laws here have as their permutations transpositions or products of disjoint transpositions. We also know from the above discussion of the use of the substitution rule (2.6) what kind of law $\ell^{(k)}$ is a consequence of shorter laws: it is one that switches the variables $x_{i+1}, x_{i+2}, \ldots, x_m$ and $x_{m+i}, x_{m+i+1}, \ldots, x_{n-1}$ as complete blocks, where $i \leqslant m-2$, that is to say the blocks contain at least two variables: x_{m-1} and x_m are always moved together, and exchanged for the pair x_{n-2}, x_{n-1}. Thus no sequence of laws $\ell^{(k)}$ can link w_n and w'_n.

Thus we have shown the following fact.

Theorem 6.2. *Each of the laws*

$$\ell'_n: \qquad w_n = w'_n$$

for even $n = 2m \geqslant 6$ is independent of all shorter laws.

We remark that we could have used the same arguments to show that the laws

$$\ell''_n: \qquad w_n = w''_n,$$

where w''_n is obtained from w_n by interchanging x_m and x_{n-1}, are independent of all shorter laws; but ℓ''_n is a consequence of ℓ'_n and the law

$$\ell^*_n: \qquad w_n = w^*_n,$$

where w^*_n is obtained from w_n by interchanging both x_{m-1} and x_{n-2} and x_m and x_{n-1}; and ℓ^*_n is a consequence of the shorter law ℓ''_{n-1}, using (2.6).

We are now ready to prove our main result.

Theorem 6.3. *The laws of $\mathscr{G}$ have no finite basis.*

Proof. This is an easy corollary of Theorem 6.2; for let $\mathscr{L}$ be some finite set of laws of $\mathscr{G}$ and λ be the length of the longest law in $\mathscr{L}$. Choose an even number n that is strictly greater than λ. Then the law ℓ'_n is independent of $\mathscr{L}$. □

The infinite sequence of laws $\ell'_6, \ell'_8, \ldots$, together with the medial law, does not form a basis of the laws of $\mathscr{G}$; it appears that a basis of the laws will have to contain an increasing number of laws of length n with increasing even n. We also leave open the question whether a basis of the laws of $\mathscr{G}$ can consist of only transposition laws.

References

[1] I.M.H. Etherington, Non-associative arithmetics, Proc. Roy. Soc. Edinburgh, Sect. A 62 (1949) 442–453.
[2] A.C. Kim, Laws in groupoids derived from semigroups, Bull. Austral. Math. Soc. 26 (1982) 385–392.
[3] D.C. Murdoch, Quasi-groups which satisfy certain generalized associative laws, Amer. J. Math. 61 (1939) 509–522.